

ABSTRACT OF THE DISCLOSURE

A method, system, and article of manufacture to share trusted hardware across multiple operational environments. A virtual machine monitor (VMM) is loaded to support a plurality of virtual machines in a computer system, the VMM including a VMM multiplexer. A first and second virtual machine (VM) are loaded. A trusted hardware device is shared between the first VM and the second VM using the VMM multiplexer. In one embodiment, the trusted hardware device includes a trusted platform module (TPM).